ABSTRACT

A distributed multi-agent system and method is implemented and employed across at least one intranet for purposes of real time collection, monitoring, aggregation , analysis and modeling of system and network operations, communications, internal and external accesses, code execution functions, network and network resource conditions as well as other assessable criteria within the implemented environment. Analytical models are constructed and dynamically updated from the data sources so as to be able to rapidly identify and characterize conditions within the environment (such as behaviors, events, and functions) that are typically characteristic with that of a normal state and those that are of an abnormal or potentially suspicious state. The model is further able to implement statistical flagging functions, provide analytical interfaces to system administrators and estimate likely conditions that characterize the state of the system and the potential threat. The model may further recommend (or alternatively implement autonomously or semi-autonomously) optimal remedial repair and recovery strategies as well as the most appropriate countermeasures to isolate or neutralize the threat and its effects.